УДК 004.7

А.І. Островський
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ЗАСОБИ ТА МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В БЕЗПРОВІДНИХ МЕРЕЖАХ НА ОСНОВІ СТАНДАРТУ IEEE 802.15

A.I. Ostrovsky

METHODS AND MEANS OF INFORMATION SECURITY IN A WIRELESS NETWORK BASED ON THE STANDARD IEEE 802.15

EEE 802.15 - стандарт, який визначає фізичний шар і керування доступом до середовища для бездротових персональних мереж з низьким рівнем швидкості. Є базовою основою для протоколів ZigBee, WirelessHART та MiWi. Як альтернатива, може бути використаний спільно зі стандартом 6LoWPAN і стандартними протоколами Інтернету для побудови вбудованого бездротового Інтернету.

Основні заходи захисту систем передачі даних на базі протоколу 802.15: організація безпечних каналів аутентифікації в Bluetooth (використання алгоритму аутентифікації E1 на основі алгоритму шифрування SAFER+; шифрування даних на основі алгоритму E0 (SAFER +), управління з використанням ключів) [1]. Шифрування даних у технології 802.15 складається із чотирьох операцій: заміна першого підключа, нелінійна оборобка заміни, підміна другого підключа й лінійне перетворення. При цьому використовуються тільки байтові операції, що робить цей шифр особливо зручним для реалізації на мікропроцесорах малої розрядності. При шифруванні/дешифруванні використовується одна унімодулярна матриця розміром 16x16. Пропонується при шифруванні використати різні матриці розміром 16x16 та 32x32. Матриця може виступати елементом ключа.Основою, на якій базується безпека Bluetooth, є генерація ключів, яка виробляється на основі PIN-коду. Довжина PIN-коду може бути від 1 до 16 байт. В даний час більшість пристроїв використовує 4-байтовий код. Спочатку на основі PIN-коду за алгоритмом E2 генерується 16-байтовий Link Key, після чого за алгоритмом E3 на базі Link Key обчислюється Encryption Key. Перший ключ використовується для аутентифікації, а другий для шифрування. Існує кілька видів атак на Bluetooth-пристрої: від цілком нешкідливих - типу BlueSnarf, до повноцінних DoS-атак і міжнародних дзвінків без відома власника телефону, або "просто" викрадення СМС-повідомлень. Крім того, існують віруси, що поширюються за допомогою Bluetooth [1]. Для забезпечення конфіденційності, цілісності та доступності даних необхідно провести аудит безпеки. Для аудиту інформаційної безпеки системи передачі даних стандарту 802.15 можна використати будь-яку із спеціалізованих утиліт для виявлення та унеможливлювання спроб несанкціонованого доступу: Bluesnarfing, BlueSnarf++, BlueBug, BlueBump і т.п. [1]. За матеріалами дослідження можна надати наступні рекомендації: завжди вимикати Bluetooth після завершення передачі даних; ставити захисний код на ініціалізацію з'єднання; вмикати обов'язкову авторизацію; використовувати нестандартні і достатньо довгі за кількістю символів паролі; відхиляти будь-які запити на під’єднання з невідомими пристроями; встановити невидимий режим для будь-яких користувачів; без потреби не вмикати Bluetooth-пристрій в людних місцях; не використовувати технологію в комерційних цілях; при можливості «перепрошити» програмне забезпечення пристроїв до новіших версій.

Література

1. Bluetooth Security Vulnerabilities and Bluetooth Projects [Електронний ресурс]. - Режим доступу: URL: http://trifinite.org/trifinite_org.html